Issues with Access to Acquisition Data and Information in the Department of Defense

Executive Summary

Jessie Riposo, Megan McKernan, Jeffrey A. Drezner, Geoffrey McGovern, Daniel Tremblay, Jason Kumar, Jerry M. Sollinger

Key findings

- Government personnel and those supporting the government do not always get their first choice of data.
- Alternative sources often have data of lower quality, that are older and thus less accurate, or that are subject to a number of caveats.
- OSD analytic groups often do not have access to the originators of the data, which precludes them from going to the primary source. They may also have poor visibility of all viable data sources.
- Direct support contractors have problems similar to OSD analysts, but these problems can be compounded by laws, regulations, and policy that restrict access to certain types of information. Support contractors require special permissions to view nontechnical proprietary data.
- Data access policy is highly decentralized, not well known, and subject to a wide range of interpretation.
- The markings for unclassified information play a significant role in access. The owner or creator of a document determines what protections or markings are required. However, marking criteria are not always clear or consistently applied.
- Institutional and cultural barriers inhibit sharing.

SUMMARY ■ Acquiring military equipment is big business. The value of the current portfolio of major weapon systems is about $1.5 trillion. Managing such a large portfolio requires access to an enormous amount of acquisition data, including the cost and schedule of weapon systems (both procurement and operations), information about how they perform technically, contracts and contractor performance, and program decision memoranda. The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD[AT&L]) and those working for it need access to such data to track acquisition program and system performance and ensure that progress is being made toward such institutional goals as achieving efficiency in defense acquisition and delivering weapon systems to the field on time and on budget.

A range of organizations need access to the data for different purposes (e.g., management, oversight, analysis, administrative). Such organizations include various offices of the Department of Defense (DoD), federally funded research and development centers (FFRDCs), university-affiliated research centers (UARCs), and a host of support contractors.

But getting access to the data to carry out the analyses requested by DoD is not always easy, or, in some cases, even possible. At times, the data carry dissemination restrictions that limit their distribution. In other cases,

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Issues with Access to Acquisition Data and Information in the Department of Defense: Executive Summary	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,National Defense Research Institute,1776 Main Street, P.O. Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

proprietary information (PROPIN) is the property of a commercial firm and may not be released without that firm's explicit permission. The Office of the Secretary of Defense (OSD) asked the RAND National Defense Research Institute to identify the problems and challenges associated with sharing unclassified information and to investigate the role of policies and practices associated with such sharing. This report details the issues associated with gaining access to what is called *Controlled Unclassified Information* (CUI).

> Getting access to the data to carry out the analyses requested by DoD is not always easy, or, in some cases, even possible. At times, the data carry dissemination restrictions that limit their distribution. In other cases, proprietary information . . . is the property of a commercial firm and may not be released without that firm's explicit permission.

INITIAL STEPS DOD CAN TAKE TO FIX ACCESS PROBLEMS

Options for Improving Data Sharing

The variety of identified problems may be addressed in many ways. Each potential option requires further analysis and investigation. We offer initial thoughts to deal with the issue of access to proprietary data, as well as the general confusion regarding policy.

Options to Address the Problem of Proprietary Data Access

There are several potential options to resolve the problem of access to proprietary data.

- The Under Secretary of Defense for Acquisition, Technology and Logistics (USD[AT&L]) could seek additional billets and insource any functions that require access to proprietary data. However, this would require Office of Professional Management and congressional support.
- USD(AT&L) could seek relief through a reallocation of billets to functions that currently require access to proprietary information. This would require cross-organizational prioritization, a difficult process.
- General access could be established for all direct support contractors. This would require legislative or contractual changes. Current legislation, Title 10 U.S. Code, Section 129d, allows litigation support contractors to view proprietary information. Similar legislation might be pursued for all support contractors.
- Alternatively, additional contractual language could be placed on all DoD acquisition contracts granting support contractors restricted access to their data. The direct support contractors who receive the data would have to demonstrate company firewalls, training, personal agreements, and need to know akin to those for classified information.
- The government could seek an alternative ruling on nondisclosure requirements (NDAs), whereby blanket NDAs could be signed between the government and a direct support organization, or a company and a direct support organization, to cover multiple tasks.

Each of these options would require further analysis and coordination with Office of the General Counsel and Defense Procurement and Acquisition Policy (and Congress in the first and third options).

Options to Address Policy Confusion

There are also several options to address the confusion regarding policy.

- OUSD(AT&L) could create and maintain a central, authoritative online resource that references all relevant guidance on information management, handling, access, and release for acquisition data. This would require identifying the relevant policy and posting new policies as they become available.
- However, an online resource may not address the issue of the workforce having a general lack of expertise and insight regarding the existing policy and guidance. To cope with this problem, OUSD(AT&L) could also consider providing additional training for its staff on the identification and protection of data. This could be an annual online training for all OUSD(AT&L) staff and contractors.
- In areas where conflicting interpretations of guidance are particularly problematic, such as with For Official Use Only (FOUO) and PROPIN, additional guidance about how to determine whether information is FOUO or proprietary in the first place would be helpful. The guidance should provide specific examples of information that is considered protected, guidelines for determining whether specific information qualifies, and details regarding handling procedures for this information, including access privileges.
- Directives and incentives could be established so that markings that appear to be incorrect are challenged and not taken only on a company or individual's claim. If more-detailed determination guidance is available, it could be used to assess the validity of a marking. A process should be in place for challenging markings, and it should be exercised.

HOW THIS STUDY WAS DONE

The approach to this study had three components. The first was a policy review. Researchers reviewed DoD directives, instructions, manuals, and guides, along with executive orders, legislation, and regulations concerning information management. The objective of the review was to develop a framework for under-

standing what governs information sharing in DoD acquisition. The review included a limited number of key federal policies that might affect data sharing within DoD. A second component involved interviews with a wide range of OSD personnel involved in acquisition. Interviewers spoke with data owners, maintainers, users, and those involved with the governance of information. Interviewers also spoke with service-level acquisition personnel to determine the role that the services play in DoD data sharing. The third component involved conducting two case studies to illuminate key issues and challenges associated with data access. Both reflect the perception of several key data access issues. The first case study looks at the various central data repositories that OSD maintains and uses. More specifically, the focus was on the background, benefits, and problems associated with these repositories. The second examines the use of PROPIN in acquisition, with a particular focus on earned value data.

THE POLICY LANDSCAPE

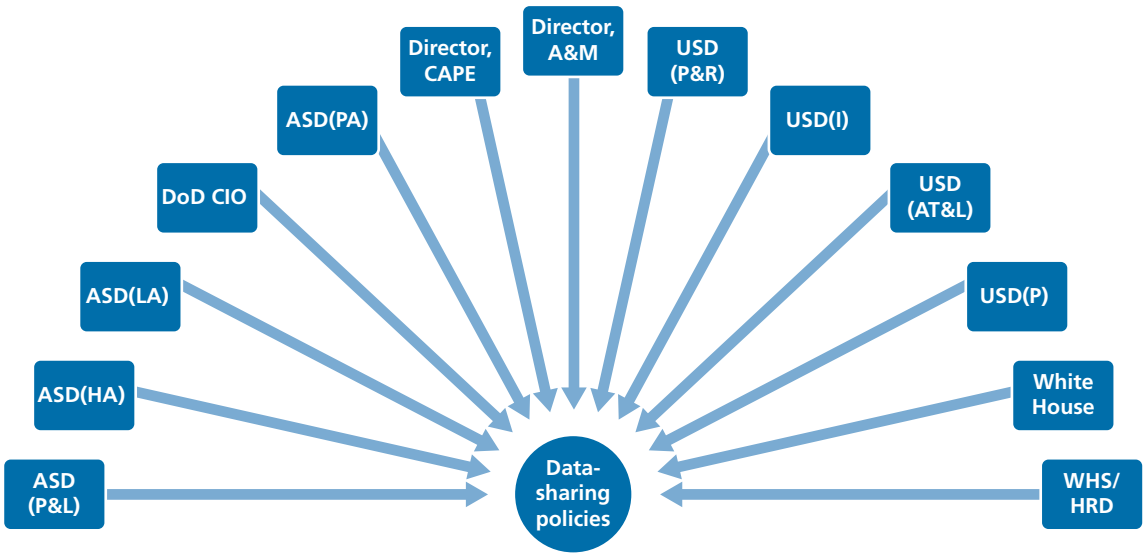
The guidance for marking and disseminating classified material is largely centralized in the *National Industrial Security Program Operating Manual.* The setting of policies for unclassified information sharing has been largely decentralized. Figure 1 indicates the many offices that play a role in determining information sharing policy.

This situation complicates an understanding of what the policies are and who has what authorities. That lack of understanding manifested itself in interviews with DoD personnel. Confusion existed about several key aspects of the policies, including what constituted a legitimate rationale for gaining access to data, who bears responsibility for removing caveats, who determines the need to know, and whether policy exists to determine where information can be disseminated. Nor did interviewees clearly understand other issues, such as what information can be considered PROPIN, who can determine that classification, and what policy governs its release.

MARKINGS

Distribution markings determine the ability of the individual possessing the information to share it with someone else. Documents that contain CUI have markings that inform users of the presence of such information. An executive order was published

Figure 1. DoD Offices Issuing Data Management, Access, Release, and Handling Policies



NOTE: Many offices are involved in making policy regarding data, and these offices change over time as a result of reorganizations. These changes often make it difficult to trace policies back to the originators. ASD(P&L) = Assistant Secretary of Defense for Production and Logistics; ASD(HA) = Assistant Secretary of Defense for Health Affairs; ASD(LA) = Assistant Secretary of Defense for Legislative Affairs; DoD CIO = DoD chief information officer; ASD(PA) = Assistant Secretary of Defense for Public Affairs; CAPE = Cost Assessment and Program Evaluation; A&M = Administration and Management; USD(P&R) = Under Secretary of Defense for Personnel and Readiness; USD(I) = Under Secretary of Defense for Intelligence; USD(AT&L) = Under Secretary of Defense for Acquisition, Technology and Logistics; USD(P) = Under Secretary of Defense for Policy; WHS/HRD = Washington Headquarters Services, Human Resources Directorate.

in 2010 that noted the inconsistent and confusing nature of procedures and policies pertaining to CUI.[1] However, the use of the CUI marking remains on hold until the phased implementation of that marking is established and markings are approved and published. In the interim, the category known as *sensitive but unclassified* (SBU) will continue to apply. Interviewees noted that two subcategories of SBU—FOUO and PROPIN—were particularly problematic. Proprietary information is discussed in one of the case studies below.

FOUO

Normally, the public can have access to federal information. *FOUO* is a marking applied to unclassified information that can be withheld from the public if disclosure would reasonably be expected to cause a foreseeable harm to an interest protected under the Freedom of Information Act (FOIA).[2] The act exempts certain information from release; an example is information classified to protect national security. In all, there are nine categories of exemptions. Requirements for and a description of FOUO information appear in DoD Manual 5200.01, Volume 4.[3] While information designated FOUO may be generally disseminated among DoD components and between DoD and contractors, consultants, grantees, and other government employees for official DoD business purposes (i.e., there is a need to know), the procedure for sharing among approved recipients may not be well known, well defined, or well understood.[4]

Other Common Markings

FOUO is but one marking that is commonly used within OSD. Other commonly found labels include *government only*, *DoD only*, *pre-decisional*, *source selection sensitive*, *business sensitive*, and *competition sensitive*. However, the origins and application procedures for many of these markings are ambiguous at best and nonexistent at worst. For example, *business sensitive* is commonly applied to information, but we could find no basis for it. We were also unable to identify what type of data has this restriction and why. Given the number of potential markings and the fog surrounding how to implement them, it would not be surprising to encounter a piece of information that one believes is improperly marked. If information is improperly marked, getting the markings changed can be challenging. The individual who placed the marking on the information must remove or change it.[5] Offices and individuals change over time, sometimes leading to confusion about who has the responsibility and authority for changing the marking if the originator of the document cannot be located or no longer feels responsible. If the originator has left the position or if the office in which the document was originally marked no longer exists, it may be difficult to find anyone else willing to take responsibility for remarking the document. If the individual is still in the office but disagrees with the suggested changes, the process for adjudicating such disagreements is unclear.

Given the number of potential markings and the fog surrounding how to implement them, it would not be surprising to encounter a piece of information that one believes is improperly marked.

PRACTICAL ISSUES AND CHALLENGES TO SHARING ACQUISITION DATA

Managing CUI requires determinations regarding the appropriate level of protection. The protection and release of information carry with them both costs and benefits. Quantifying the full range of costs is difficult. Below we highlight some of the practical issues and challenges to sharing acquisition data.

Costs of Restricting Information

The full cost of restricting, not restricting, or incorrectly restricting information is difficult to gauge. Undoubtedly, there are direct financial costs. The Information Security Oversight Office reported that the "total security classification cost estimate within Government for FY [fiscal year] 2013 is

$11.63 billion."[6] Industry is estimated to add an additional $1.07 billion. These costs are those involved in the protection and maintenance of classified information systems, physical security, personnel security (e.g., clearances, access), classification management, declassification, operations security, and training. Another direct cost is the time that people spend attempting to get access to information so they can do their jobs. This can be quite time-consuming in some cases.

A second cost is that of opportunities lost as a result of blocking the open flow of information. In fact, excessive classification "prevents federal agencies from sharing information internally[,] . . . making it more difficult to draw connections."[7] Individuals spend time, effort, and money attempting to gain access to information—which could be applied to more-productive endeavors. Furthermore, if access cannot be granted, then people rely on inferior information or data to make decisions. While the inefficiency introduced by a lack of information sharing cannot easily be translated to a monetary value, it unquestionably affects an organization's operations. Conversely, the cost of unauthorized disclosure can have significant consequences that are also tough to quantify.

Problems Accessing Data

We interviewed acquisition professionals to gain a better sense of the types of problems they run into when attempting to get or share information. Acquisition data needs were extensive but varied based on the mission of the office. Specific areas where data are needed included cost (e.g., performance, schedule, financial), test (e.g., planning, activities, execution, results), engineering (e.g., schedule, technical and performance parameters, key performance parameters/key system attributes, engineering plans), earned value (e.g., contract data and assessments, supply chain metrics, systems engineering), contract (e.g., competition, termination, funding, small-business status, list of contractors), and workforce data (e.g., position information, qualifications, tenure, assignment, promotion, waivers). The offices also needed to gather other acquisition data to support their analyses. The problems tended to differ depending on their focus. We categorized three groups: OSD functional and subject-matter experts, OSD Overarching Integrated Project Team (OIPT) or Defense Acquisition Board (DAB) review offices, and OSD analysis offices.

OSD Functional and Subject-Matter Experts

The problems the interviewees in this category noted fell into the following categories:

- latency
- political, structural, and cultural barriers to sharing
- conflicting regulations on proprietary data
- issues with utilizing structured and unstructured information in central repositories
- poor planning.

Latency refers to the time gap between when data are generated and when they are made available. If the time lag is long, those receiving the data do not get an accurate picture of the program's current status. Reasons for the lag include the need for the services to scrub data to ensure that it is accurate.

Interviewees also pointed to political, structural, and cultural barriers. Such barriers include an unwillingness to share between OSD offices. Specific political and structural issues between the services and OSD inhibited data sharing. For example, leadership may limit dissemination when organizations at lower levels want to share and vice versa. Structural "stovepipes" in OSD or the services may also inhibit data sharing because acquisition personnel tend to share more

While the inefficiency introduced by a lack of information sharing cannot easily be translated to a monetary value, it unquestionably affects an organization's operations. Conversely, the cost of unauthorized disclosure can have significant consequences that are also tough to quantify.

readily within their stovepipe or specialty rather than across functional areas. Personalities and culture also factor into the problem of sharing. For instance, the person handling the request (e.g., program office personnel, contractor, service-level management, or other personnel in the data-sharing chain) may not promote sharing or may not understand the urgency of the request. The end result is that getting the information becomes prohibitively difficult.

Interviewees frequently cited problems with proprietary information. First, it is unclear what should be considered proprietary information. That ambiguity makes it hard to push back on contractors when something may be improperly labeled *PROPIN*. Given the restrictions on PROPIN data and the legal liability for the mishandling of such data, some interviewees noted that they exercise more care in handling PROPIN materials. Others expressed less concern about legal liability. A related problem is that NDAs are required of people outside the government handling these data, and it is sometimes difficult to get NDAs signed in a timely fashion (e.g., parties involved want to add additional clauses) or at all if a support contractor is considered to be a competitor of the prime contractor that "owns" the data.

Information stored in central repositories poses a separate set of issues. Although these repositories are generally regarded as useful, they may not be useful for all who want to benefit from them because they need to be updated, and funding for updates may not be available. Various business rules may also limit access. Additionally, they tend to limit real-time access to data until they are properly processed, described, or checked for accuracy. And, sometimes, they duplicate other databases, making it unclear which one is authoritative. Furthermore, processes for getting access to central repositories are not always the same (meaning that repositories use a variety of business rules and information technology–related measures for access). Some require a Common Access Card (CAC), while others require username and login only. Still others require a CAC and allow access only from a military network.

Finally, poor planning makes it difficult to retrieve data. Acquisition personnel may not plan ahead or anticipate future data needs. When data-reporting requirements are not properly added to a contract up front, the government must negotiate with contractors for these data. This can be costly for the government and particularly detrimental when budgets are tight. Furthermore, if contracts contain the wrong clauses, then the government must either modify the contract or find other means to get the data.

It is unclear what should be considered proprietary information. That ambiguity makes it hard to push back on contractors when something may be improperly labeled *PROPIN*.

OSD OIPT or DAB Review Offices

Interviewees in this category were heavily involved in DAB meeting preparation and reviews and in developing defense acquisition executive summaries (DAESs). Interviewees also analyze the portfolios of the acquisition programs for which they have responsibility for oversight; perform program oversight through the review of draft program planning and milestone documentation; and participate in program reviews, technical readiness assessments, and other reviews that reflect on program performance and are part of the oversight process.

This group reported a range of data access or handling problems. Lack of access to comptroller databases that contain procurement and research, development, test, and evaluation budget details makes it difficult to gather budgeting information for portfolio analyses. Others noted that programs are more likely to share data and information when things are going well but less likely to do so if a program is encountering execution problems.

Interviewees also noted access problems for support contractors working in the OSD OIPT or DAB review offices with respect to documents in the Acquisition Information Repository (AIR). Part of the issue is that document owners can specify access constraints when uploading their documents to AIR, which means that a document owner can deny access regardless of the specific rationale for the request. Furthermore, each document or type must be requested individually, a disincentive for using the repository.

Combining unclassified data that reside on both the Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet) can be problematic. If unclassified information is posted on the SIPRNet but is needed on the NIPRNet, the process for moving the data from one to the other is complex. Interviewees also noted inconsistencies in data from different sources. Furthermore, many offices did not want to grant access to internal systems, because the data exist in multiple formats and are still raw data that need to be reviewed to ensure that they do not contain errors.

OSD Analysis Offices

Interviewees in the analysis-oriented offices said that they need access to the full spectrum of data, cutting across both functional areas and programs, including program documentation, planning materials, briefings, and information that enables an understanding of the cost, schedule, and performance of programs or portfolios of programs.

Handling data marked *PROPIN* or *FOUO* was problematic, according to interviewees in the analysis-oriented offices, in large part because the criteria used to mark documents were neither transparent nor consistent across types of documents and data owners. The upshot is that different documents with the same information may be marked differently. Interviewees recounted presenting unclassified information that had been approved for public release at conferences and later seeing that same information marked *PROPIN* in a contractor's presentation. Proprietary information is protected by law, but interviewees noted that few understand how the law applies in specific cases.

Stovepipes, both within OUSD(AT&L) and among external organizations, were also identified as a constraint on sharing data, including access approval. Organizations tend to assist others who have the same specific mission or role before assisting those asking for information outside their mission. Most interviewees recognized bureaucratic impediments for sharing data, including the fact that only a few people can authorize access, while many can block it. Additionally, program offices generally require some level of approval before they can release data, which delays full disclosure or data sharing outside the office until approvals are completed. Interviewees noted that it was typically easier to get information from OSD sources than from the services if they did not have an established contact.

CASE STUDY: PROBLEMS ACCESSING CENTRALIZED DATA REPOSITORIES

OSD has several central repositories that house a range of acquisition information that is useful for execution, oversight, and analysis. Researchers reviewed seven repositories:

- AIR
- Defense Acquisition Management Information Retrieval (DAMIR)
- Defense Automated Cost Information Management System (DACIMS)
- Defense Technical Information Center (DTIC)
- Federal Procurement Data System–Next Generation (FPDS-NG)
- Performance Assessments and Root Cause Analyses's (PARCA's) Earned Value Management Central Repository (EVM-CM)
- OUSD(AT&L)'s Workforce Data Mart.

The repositories hold acquisition information from the 46 information requirements defined by the current Department of Defense Instruction (DoDI) 5000.02.[8] They also include more-detailed cost, budget, earned value, scientific, technical, engineering, contract, and workforce data. The typical procedure is to have a "trusted agent" or government sponsor who will vouch for the need for access to certain information. Government employees always have an easier time getting access than contractors, because government employees are presumed to have a need to know because of their official function. The use of a DoD CAC or public key infrastructure (PKI) is also normally required for access. Table 1 describes the databases.

Problems Identified by Interviewees

Interviewees cited multiple problems with accessing and utilizing central repositories for their work. For example, the various repositories have many scanned documents. Depending on the format, scanned documents are difficult to search (i.e., some are images only that have not been converted to searchable text). Because repositories have grown very large, those that allow queries are more useful than those that do not. Interviewees also stated that not all of their data needs are met by central repositories, which may not have the resources to include everything requested. Prioritizing data needs and capabilities for a central repository will inevitably leave some analysts without all the capabilities that they need. It was

Table 1. OSD Central Repositories

	AIR	DAMIR	DACIMS	DTIC	FPDS-NG	EVM-CR	Workforce Data Mart
Content	Acquisition information required by the current DoDI 5000.02 (46 information requirements) and an acquisition decision memorandum by USD(AT&L).	Selected acquisition reports, Major Automated Information Systems Annual Report, acquisition program baselines, defense acquisition executive summaries, program objective memoranda, budget estimate submissions, president's budgets, major automated information system annual and quarterly reports, top-level earned value data.	Current and historical cost and software resource data needed to develop independent, substantiated estimates. Includes almost 30,000 Contractor Cost Data Reports, Software Resources Data Reports, and associated documents.	DoD- and government-funded scientific, technical, engineering, and business information available today (public, FOUO, and classified)	Information about federal contracts; allows reporting on federal contracts. Contracts whose estimated value is $3,000 or more. Every modification to that contract, regardless of dollar value, must be reported to FPDS-NG.	Detailed earned value data.	Acquisition workforce data.
Year started	2012	2004–2005	1998	1945	1978 (as FPDS)	2008 in Defense Cost and Resource Center (DCARC)	2008
Access adjudicator	Office that approves document	Acquisition Resources and Analysis (ARA)	OSD Cost Assessment and Program Evaluation (CAPE)	Originator of the data	General Services Administration (GSA)	PARCA	Human Capital Initiative (HCI)
Repository manager	ARA	ARA	OSD CAPE	DTIC	GSA	PARCA	HCI
Repository host	DTIC	DoD Washington Headquarters Services, the Enterprise Information Technology Services Directorate (EITSD)	OSD CAPE	DTIC	GSA	OSD CAPE	Defense Acquisition University (DAU)

Another concern of interviewees was that there was not a centralized or authoritative process for scrubbing and validating all data in a given repository, which may lead to inconsistencies across repositories.

mentioned that many central repositories lack OSD-level pre-Major Defense Acquisition Program (MDAP) information and testing data. In addition, the process of building and populating central repositories takes years. AIR started in 2012 and has been somewhat populated, but there are still more documents that need to be added. Depending on what is provided, it can take a considerable amount of time for personnel to upload all required information—in other words, to institutionalize the process of uploading data to repositories.

Interviewees also agreed on the point that it takes a long time to master using the various central repositories because the software and structure are often very different across databases.

Because of this, some interviewees reported that they did not access these repositories regularly, or they relied heavily on staff members with better knowledge of the databases. Some analysts were also unaware of all the available repositories and, consequently, did not know which data could be accessed. Acquisition personnel were aware of the repositories but did not fully use them, or they perceived access and permission as too time-consuming to pursue. In addition, for multiple reasons, there was sometimes a preference for receiving information through working relationships with peers.

Another concern of interviewees was that there was not a centralized or authoritative process for scrubbing and validating all data in a given repository, which may lead to inconsistencies across repositories. In addition, we heard that people or organizations within DoD or contractor organizations are generating data but are not willing to post this information in a repository.

Finally, the use of central repositories as a means of storing, sharing, and analyzing data has increased in DoD over time. The owners of those repositories are faced with a myriad of challenges related to sharing, including integrating information assurance and security policies and procedures, along with business rules, into the architecture of the systems. They also must integrate verification of who can and cannot access which data in the systems. Approving access is not a trivial task, with the thousands of potential users who want access. From the standpoint of those managing repositories, another problem identified during our interviews was that the process of retrofitting systems after the introduction of new security policies or business rules tends to be very cumbersome and time-consuming. One such example involved trying to deal with accounts that become inactive after a certain period of time as dictated by policy. Another was adding a security requirement after the security architecture was defined.

CASE STUDY: PROPRIETARY DATA

Interviewees frequently cited issues with information labeled "proprietary." The purpose of this case study is to clarify what we mean by *proprietary data*, identify key legal and regulatory regimes that govern the use and protection of proprietary data, and review some notional situations in which the use of proprietary data could cause logistical difficulties for offices whose analysis relies on contractor-provided proprietary information. Note that while of great interest to those who need access to it, proprietary data is but one example of the complicated environment that arises when data, regulations, workforce demographics, and the demands of business and policy interact.

What Is Proprietary Information?

Proprietary information, labeled PROPIN on documents that contain it, are data that someone outside the government has both generated and wants to keep private for business reasons. A raft of information can be considered PROPIN: copyrights, patents,[9] trademark and trade secrets, and business practices, processes, and finances. This information provides a business with a competitive advantage or otherwise contributes to profitability, viability, and success.

DoDI 5230.24 defines *proprietary information* as follows: "Information relating to or associated with a company's products, business, or activities, including, but not limited to, financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and knowledge that have been clearly identified and properly marked by the company as 'proprietary information,' trade secrets, or company confidential information."[10] Note that the company itself, not DoD, labels information as proprietary and thereby triggers the protections (both DoD and legal) that govern its use and distribution beyond DoD. One further caveat to the definition is worth noting: "The information must have been developed by the company and not be available to the Government or to the public without restriction from another source."[11] Here, the government stresses that the company must have developed the information that it seeks to label as PROPIN.

What Legal and Regulatory Regimes Govern Proprietary Information?

The PROPIN label triggers safeguards and potential legal penalties for the mishandling of the information. When a company has labeled information as PROPIN, the recipient must protect the data from intentional release to the public or other unauthorized users. The Trade Secrets Act governs proprietary information. Something of a misnomer, the Trade Secrets Act is a catchall term that applies to a series of state and federal laws governing commercial secrets. Because DoD deals with companies and nonprofits that may fall under the jurisdiction of state law, both federal and state protections for trade secrets and proprietary information apply. The Economic Espionage Act of 1996 further enforces the protection of trade secrets by making their misappropriation a federal offense.[12] Furthermore, 18 U.S.C. 1905 contains additional legal rules and criminal penalties specifically associated with federal government employees who disclose confidential (nonclassified) information. Besides these legal restrictions on the release of proprietary data, DoD has issued rules for the marking and handling of information marked *PROPIN*, spelled out in DoD Manual 5200.01, Volume 4.

Situations That Cause Problems for Those Relying on Proprietary Information

To understand why contractor support causes problems for DoD when handling PROPIN data, we present a series of stylized graphics that depict the flow of information in scenarios in which the government requires contractor-supplied data. These generic scenarios are meant to highlight the broad areas of concern about whether data are available to the government or whether the nature of the government's workforce (i.e., government employee compared with contractor support) hinders timely access to data.

Figure 2 depicts the flow of data within DoD, which regularly and routinely handles PROPIN data. Typically, the government has contracted with an outside provider (labeled here the prime contractor) that furnishes the data to the government on a restricted basis. The program office receives these data and works with OSD staff to analyze and examine program progress. The data are furnished by the contractor and, in accordance with DoD policy, must be marked by the contractor as PROPIN. Furthermore, only government employees in both OSD and the program office can handle the data.

Figure 2. Problematic Proprietary Data Flows (Scenario 1)

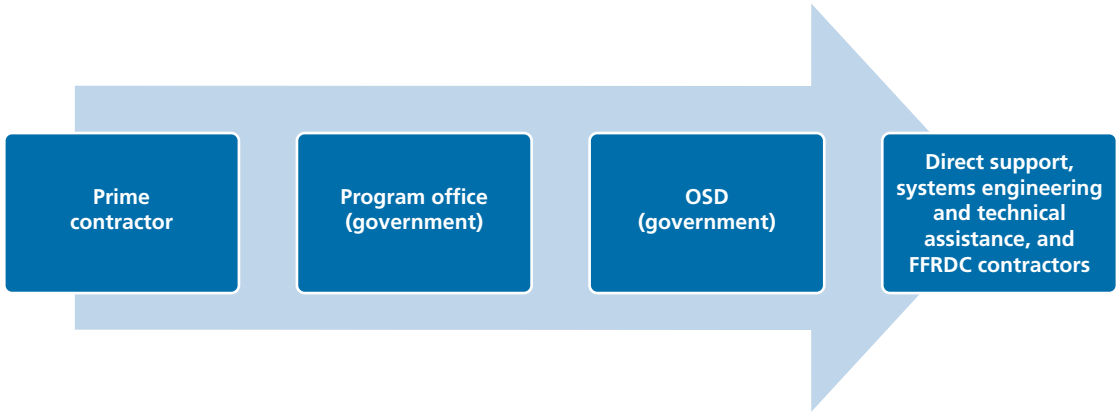
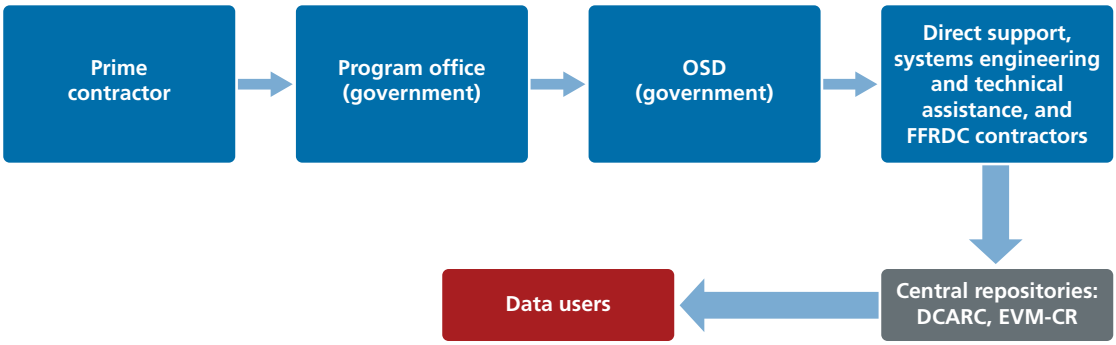


Figure 3. Problematic Proprietary Data Flows (Scenario 2)



If only government employees staff the offices, there is no concern about handling PROPIN information. But complications arise when we relax the assumption of government employees constituting the staff of the program and OSD offices. Because the offices rely, sometimes heavily, on the support of contractors to perform analysis, some offices likely seek to distribute analytic tasks that call for prime contractor–provided PROPIN data to support contractors. On the right side of Figure 2, we identify direct support, systems engineering and technical assistance, and FFRDC contractors to represent the types of secondary contractors that might be called on to carry out these analytic tasks. Because PROPIN rules, before 2013, stated that the government may not release such information to the public or unauthorized third parties, it would seem that the government may not employ support contractors for analytic tasks using PROPIN data, and thus the rules hamper the flow of data.

> DoD has several repositories that store proprietary data. Burdensome access requirements would either stifle the flow or drive contractors to use less accurate but more accessible data.

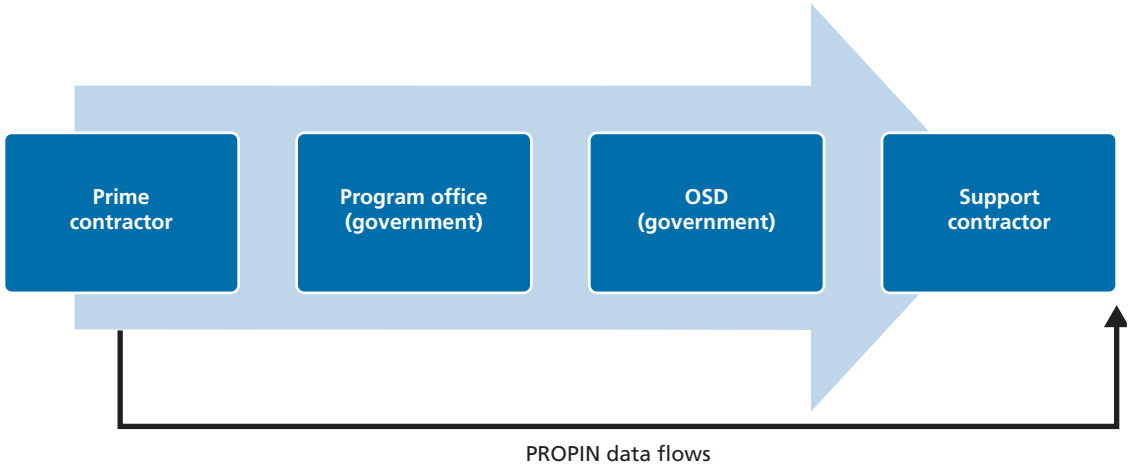
To get the best use from analytic support contractors, the government would need specific permission from the prime contractor to grant access to contractor support staff. Likely, this would take the form of an NDA, a document that would grant access to a specific contractor (or perhaps even a specific employee of a contractor) for specific pieces of information for a specific period. This process, according to our interviews, was a burdensome task and one of questionable efficacy. Should the prime contractor perceive the support contractor as a competitor, it could deny permission to use the data.

Figure 3 presents a variation on the situation depicted in Figure 2. Here, the PROPIN data are stored in a central repository. This scenario assumes that those who uploaded the data into the repository had permission to handle the PROPIN data.

Once the PROPIN data are in the central repository, however, questions arise about who—beyond government employees—may have access to the central repository or who manages the data in the repository, as well as about how access may be granted. Since the central repository may have data from many prime contractors, support contractors seeking access may encounter significant challenges. For example, if any access to the repository means access to all its data, would contractors need NDAs with every prime contractor whose PROPIN data were stored in the repository? Questions of access and monitoring are not merely academic. DoD has several repositories that store proprietary data. Burdensome access requirements would either stifle the flow or drive contractors to use less accurate but more accessible data.

Figure 4 depicts a somewhat less likely but still possible situation concerning PROPIN data flows that can arise if the

Figure 4. Problematic Proprietary Data Flows (Scenario 3)



government itself is kept out of the loop. This might occur if the prime and support contractors solve the access issue by transferring the data directly. In this case, the data flow from the prime contractor to the support contractor, thus eliminating the government's oversight, direction, and visibility of the data. In this scenario, the government may be able to obtain the analysis it needs in a timely fashion, but it potentially loses its own access to the data.

Faced with concern about government offices being hamstrung by a myriad of NDAs, Congress revised regulations surrounding the role of government support contractors and access to PROPIN data. As part of the National Defense Authorization Act of 2010, Congress defined government support contractors as those on a contract with the government, "the primary purpose of which was to furnish independent or impartial advice or technical assistance directly to the government."[13] In our scenarios, the support contractors would likely qualify as government support contractors under the new definition. These newly defined contractors, according to the 2010 law, would have access to proprietary information, subject to legal restrictions regarding transmission to the public or unauthorized third parties. This, essentially, would put government support contractors on par with government employees for the purpose of accessing the proprietary information necessary to fulfill the government support contract. As a result, government support contractors can now have "access to and use of any technical data delivered under a contract for the sole purpose of furnishing independent and impartial advice or technical assistance directly to the Government in support of the Government's management and oversight of the program or effort to which such technical data relates."[14]

In 2013, there was also a revision to the Defense Federal Acquisition Regulation Supplement (DFARS). It would seem that the revision to DFARS concerning government support contractors would resolve concerns about data flow and access. Yet the revision pertains to government support contractors and *technical data*. A term defined in law, *technical data* refers to a raft of regulations in DFARS 252.227. Without going into the technicalities of the definition, it should suffice to mention that earned value management (EVM) data—financial data used to measure whether programs' cost and performance are on schedule—fall into a gray area that does not fit squarely within the DFARS definition of *technical data*.

This ambiguity raises precisely the sorts of questions outlined in Figures 2 and 3, in which support contractors deployed to work with EVM data cannot do so because the new regulation does not seem to apply (because the law only refers to access to "technical data").

Furthermore, because the regulations do not clearly establish the nature of EVM data, it is not clear whether these are technical data or financial data. Hence, whereas the Federal Acquisition Regulations and DFARS regulations provide clear guidance regarding data rights for technical data—including remedies for inappropriately restricted data and access to technical data by government support contractors—the regulations do not provide corresponding guidance regarding data rights for financial or management information, such as EVM data.

In sum, the PROPIN environment has created a situation whereby the government has initially restricted contractor access to PROPIN data, then subsequently begun a patchwork process of granting access in limited circumstances. But the patchwork process is incomplete. EVM data represent only one

of potentially many types of nontechnical data that government offices use. To the extent that these offices rely on contractor support for their data management and analysis, they may be barred from doing so until similar revisions to the Federal Acquisition Regulations and DFARS are approved.

CONCLUSIONS

The problems with access to DoD acquisition data are many and varied. Significant confusion exists on the part of those who possess acquisition information and those who need it to do their jobs. The result is analysis that takes longer than it should, costs more than it should, and often uses data that are not the best, leading to lower-quality analysis. There are important reasons for restricting access, which require balancing control with granting more access. In information assurance and security policy, there is an understanding that no individual should have unfettered access to all data. Given the inherent complexity in securing data and sharing data, any solutions to problems associated with data-sharing challenges should be well thought out to avoid the multitude of unintended consequences that could arise.

Given the inherent complexity in securing data and sharing data, any solutions to problems associated with data-sharing challenges should be well thought out to avoid the multitude of unintended consequences that could arise.

Notes

[1] Executive Order 13556, *Controlled Unclassified Information*, Washington, D.C.: The White House, November 4, 2010.

[2] The Freedom of Information Act of 1966, as amended by United States Code, Title 5, Section 552, Public information; Agency Rules, Opinions, Orders, Records, and Proceedings, January 16, 2014.

[3] U.S. Department of Defense Manual 5200.01, Vol. 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, February 24, 2012.

[4] Despite the FOUO guidance, many interviewees did not understand when FOUO should be applied and who was able to view FOUO information.

[5] DoD Manual 5200.01, 2012, states, "The originator of a document is responsible for determining at origination whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings. . . . The originator or other competent authority (e.g., initial FOIA denial and appellate authorities) shall terminate the FOUO status of specific information when circumstances indicate that the information no longer requires protection from public disclosure."

[6] Information Security Oversight Office, *2013 Report to the President*, Washington, D.C.: U.S. National Archives and Records Administration, 2014, p. 22.

[7] Elizabeth Goitein and David M. Shapiro, *Reducing Overclassification Through Accountability*, New York: Brennan Center for Justice, NYU School of Law, 2011, p. 1.

[8] U.S. Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015.

[9] Patents are publicly accessible, but the technology cannot be used without agreement from the patent holder.

[10] DoDI 5230.24, *Distribution Statements on Technical Documents*, August 23, 2012, p. 29; emphasis added.

[11] DoDI 5230.24, 2012, p. 29.

[12] 18 U.S.C. 1832.

[13] U.S. Congress, 111th Cong., National Defense Authorization Act for Fiscal Year 2010, Washington, D.C., H.R. 2647, Public Law 111–84, October 28, 2009, Section 821.

[14] U.S. Department of Defense, Defense Federal Acquisition Regulation Supplement, Government Support Contractor Access to Technical Data (DFARS 2009-D031), *Federal Register*, Final Rule, May 22, 2013.

About This Report

This research was sponsored by the Office of the Secretary of Defense (OSD) and conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND Acquisition and Technology Policy Center, see http://www.rand.org/nsrd/ndri/centers/atp.html or contact the director (contact information is provided on the web page).

We thank the sponsors of this study: Mark Krzysko, deputy director of enterprise information, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Acquisition Resources and Analysis Directorate (OUSD[AT&L]/ARA); Steven Miller, director, Advanced Systems Cost Analysis Division, OSD, Cost Assessment and Program Evaluation (CAPE); and Gordon Kranz, deputy director, Earned Value Management, OUSD(AT&L)/Performance Assessments and Root Cause Analysis. We would also like to thank our project monitor, Jeff Tucker, acquisition visibility capability manager, OUSD(AT&L)/ARA, for his guidance and support throughout this study. We thank the following people who provided us with additional background information that informed our analysis: Douglas Shontz; Chad Ohlandt; Larrie Ferreiro, director of research, Defense Acquisition University; Rob Flowe, OSD Studies and Federally Funded Research and Development Center Management, OUSD(AT&L)/ARA; and Bess Dopkeen, Advanced Systems Cost Analysis Division, OSD CAPE. We'd also like to thank the Acquisition Visibility team and everyone else who volunteered their valuable time to describe their points of view to the RAND study team. We are also grateful to the contractors Brian Baney and Melissa Tengs, who helped facilitate communication with the Office of Enterprise Information in OUSD(AT&L)/ARA.

About the Principal Investigators

Jessie Riposo is a senior operations researcher at RAND with experience in research and analysis and a specialty in defense acquisition and planning, programming, and budgeting.

Megan McKernan is a senior project associate predominantly working in DoD acquisition.

Limited Print and Electronic Distribution Rights

For more information on this publication, visit www.rand.org/t/rr880z1.

www.rand.org

RR-880/1-OSD